

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード* (参考)
G 0 6 F 3/12		G 0 6 F 3/12	D 2 C 0 6 1
B 4 1 J 29/38		B 4 1 J 29/38	Z 5 B 0 2 1
G 0 6 F 13/00	3 5 7	G 0 6 F 13/00	3 5 7 A 5 B 0 8 9

審査請求 未請求 請求項の数 6 O L (全 8 頁)

(21) 出願番号 特願平11-183407

(22) 出願日 平成11年6月29日 (1999.6.29)

(71) 出願人 000006747

株式会社リコー

東京都大田区中馬込1丁目3番6号

(72) 発明者 渡邊 義昭

東京都大田区中馬込1丁目3番6号 株式会社リコー内

Fターム(参考) 2C061 AP01 HJ08 HQ12 HQ17

5B021 AA01 EE04 NN18

5B089 GA13 KA03 KB04 KB06 KB13

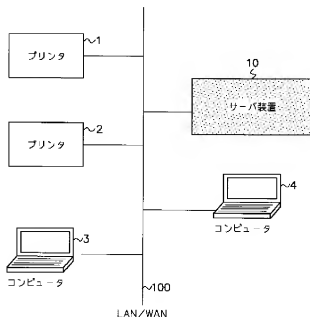
LB12

(54) 【発明の名称】 プリンタアクセス制御システム

(57) 【要約】

【課題】 ネットワーク接続された複数のプリンタのアクセス制限の設定を容易に行うことができるプリンタアクセス制御システムを提供する。

【解決手段】 サーバ装置10に、複数のプリンタをグループ化して登録したプリンタ管理テーブルを管理するプリンタグループ管理部27と、プリンタのグループ毎にユーザ情報を登録したプリンタアクセス管理テーブルを管理し、P C装置からの印刷要求に含まれる印刷依頼プリンタが、プリンタグループ管理部27の管理するプリンタ管理テーブルに含まれていない場合、またはP C装置からの印刷要求に含まれるユーザ名が、プリンタアクセス管理テーブルに登録されていない場合に、P C装置からの印刷要求を拒否するアクセス制限処理部26とを備えたことにより、ネットワーク上の複数のプリンタのアクセス制限をサーバ装置上で行うことができ、アクセス条件設定の作業効率を向上させることができる。



## 【特許請求の範囲】

【請求項1】 印刷要求を出力する印刷クライアント装置と、

前記印刷クライアント装置からの印刷要求に含まれる印刷データを蓄積し、プリンタ装置に蓄積した印刷データを送信するサーバ装置と、

前記サーバ装置から送られてきた印刷データを記録手段により用紙に記録出力するプリンタ装置とがネットワークに接続されたプリンタアクセス制御システムであって、

前記サーバ装置は、

前記ネットワークに接続された複数のプリンタ装置をグループ化して登録したプリンタ管理テーブルを管理するプリンタグループ管理手段と、

前記プリンタ装置のグループ毎にユーザ情報を登録したプリンタアクセス管理テーブルを管理し、前記印刷クライアント装置からの印刷要求に含まれる印刷依頼プリンタ装置が、前記プリンタグループ管理手段の管理するプリンタ管理テーブルに含まれていない場合、または前記印刷クライアント装置からの印刷要求に含まれるユーザ名が、前記プリンタアクセス管理テーブルに登録されていない場合に、前記印刷クライアント装置からの印刷要求を拒否するアクセス制限手段と、

を有することを特徴とするプリンタアクセス制御システム。

【請求項2】 前記サーバ装置は、

複数のユーザ名をグループ化して登録したユーザグループ管理テーブルを管理するユーザグループ管理手段を有し、

前記アクセス制限手段は、

前記印刷クライアント装置からの印刷要求に含まれる印刷依頼プリンタ装置が、前記プリンタグループ管理手段の管理する前記プリンタ管理テーブルに含まれていない場合、または前記印刷クライアント装置からの印刷要求に含まれるユーザ名が、前記プリンタアクセス管理テーブル及び前記ユーザグループ管理テーブルに登録されていない場合に、前記印刷クライアント装置からの印刷要求を拒否することを特徴とする請求項1記載のプリンタアクセス制御システム。

【請求項3】 前記サーバ装置は、

登録されたユーザのパスワード情報を登録したパスワード情報テーブルを管理するユーザ情報管理手段を有し、

前記アクセス制限手段は、

前記印刷クライアント装置からの印刷要求に含まれる印刷依頼プリンタ装置が、前記プリンタグループ管理手段の管理する前記プリンタ管理テーブルに登録され、前記印刷クライアント装置からの印刷要求に含まれるユーザ名が、前記プリンタアクセス管理テーブルに登録され、前記印刷クライアント装置からの印刷要求に含まれるパ

スワードが、前記ユーザ情報管理手段の管理するパスワード情報テーブルに登録されていた場合に、前記印刷クライアント装置からの印刷要求を受理することと特徴とする請求項1記載のプリンタアクセス制御システム。

【請求項4】 前記サーバ装置は、

登録されたユーザのパスワード情報を登録したパスワード情報テーブルを管理するユーザ情報管理手段を有し、前記アクセス制限手段は、

前記印刷クライアント装置からの印刷要求に含まれる印刷依頼プリンタ装置が、前記プリンタグループ管理手段の管理する前記プリンタ管理テーブルに登録され、

前記印刷クライアント装置からの印刷要求に含まれるユーザ名が、前記プリンタアクセス管理テーブルに登録されているか、または前記ユーザグループ管理手段の管理するユーザグループ管理テーブルに登録され、

前記印刷クライアント装置からの印刷要求に含まれるパスワードが、前記ユーザ情報管理手段の管理する前記パスワード情報テーブルに登録されていた場合に、前記印刷クライアント装置からの印刷要求を受理することと特徴とする請求項2記載のプリンタアクセス制御システム。

【請求項5】 複数のプリンタと、

印刷処理実行不可能なプリンタ装置の情報であるアクセス制限情報を管理するサーバ装置と、

前記サーバ装置から前記アクセス制限情報を取得し、このアクセス制限情報に基づいて、印刷要求を出力するプリンタ装置を選択する印刷クライアント装置と、  
がネットワークに接続されていることを特徴とするプリンタアクセス制御システム。

【請求項6】 前記印刷クライアント装置は、所定の間隔毎に前記サーバ装置の管理する前記アクセス制限情報を取得する取得手段と、

前記取得手段にて取得した前記アクセス制限情報を記憶する記憶手段と、

を有することを特徴とする請求項5記載のプリンタアクセス制御システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワーク接続されたプリンタのプリンタアクセス制御システムに関する。

【0002】

【従来の技術】従来、複数のワークステーションにより構築されたネットワークにネットワークプリンタとして接続されたプリンタのアクセス制御は、例えば、どのユーザに対してプリンタの使用を許可するかを決定するアクセス権の有無により指定されていた。しかし、このシステム制御では、許可されているユーザ毎の細かな条件を設定することができなかった。

【0003】この問題を解決する方法として、特開平8

ー31468号公報では、プリンタにユーザ名を、アクセス権を示す情報として登録し、同時にそのユーザ毎の記録出力の制限をするプリンタアクセス情報を登録することにより、ユーザ毎のより細かな制御を行うネットワークプリンタ装置を提案している。

#### 【0004】

【発明が解決しようとする課題】しかしながら、このネットワークプリンタ装置では、ネットワーク接続された複数のプリンタを同一の条件でアクセス制限を行う場合には、同じ操作をそれぞれのプリンタに対して行わなければならないため、大変手間がかかり、作業効率が悪くなるという問題が発生していた。

【0005】また、ネットワーク上に存在するサーバ装置上からアクセス制限を行う場合、サーバ経由の印刷のみしかアクセス制限が行えないという問題も有していた。

【0006】本発明は、従来の欠点を解消し、ネットワーク接続された複数のプリンタのアクセス制限の設定を容易に行うことができるプリンタアクセス制御システムを提供することを目的とする。

#### 【0007】

【課題を解決するための手段】かかる目的を達成するために、本発明のプリンタアクセス制御システムは、印刷要求を出力する印刷クライアント装置と、印刷クライアント装置からの印刷要求に含まれる印刷データを蓄積し、プリンタ装置に蓄積した印刷データを送信するサーバ装置と、サーバ装置から送られてきた印刷データを記録手段により用紙に記録出力するプリンタ装置とがネットワークに接続されたプリンタアクセス制御システムであって、サーバ装置は、ネットワークに接続された複数のプリンタ装置をグループ化して登録したプリンタ管理テーブルを管理するプリンタグループ管理手段と、プリンタ装置のグループ毎にユーザ情報を登録したプリンタアクセス管理テーブルを管理し、印刷クライアント装置からの印刷要求に含まれる印刷依頼プリンタ装置が、プリンタグループ管理手段の管理するプリンタ管理テーブルに含まれていない場合、または印刷クライアント装置からの印刷要求に含まれるユーザ名が、プリンタアクセス管理テーブルに登録されていない場合に、印刷クライアント装置からの印刷要求を拒否するアクセス制限手段とを有することを特徴とする。

【0008】上記のサーバ装置は、複数のユーザ名をグループ化して登録したユーザグループ管理テーブルを管理するユーザグループ管理手段を有し、アクセス制限手段は、印刷クライアント装置からの印刷要求に含まれる印刷依頼プリンタ装置が、プリンタグループ管理手段の管理するプリンタ管理テーブルに含まれていない場合、または印刷クライアント装置からの印刷要求に含まれる

ユーザ名が、プリンタアクセス管理テーブル及びユーザグループ管理テーブルに登録されていない場合に、印刷クライアント装置からの印刷要求を拒否するとい。

【0009】上記のサーバ装置は、登録されたユーザのパスワード情報を登録したパスワード情報テーブルを管理するユーザ情報管理手段を有し、アクセス制限手段は、印刷クライアント装置からの印刷要求に含まれる印刷依頼プリンタ装置が、プリンタグループ管理手段の管理するプリンタ管理テーブルに登録され、印刷クライアント装置からの印刷要求に含まれるユーザ名が、プリンタアクセス管理テーブルに登録され、印刷クライアント装置からの印刷要求に含まれるパスワードが、ユーザ情報管理手段の管理するパスワード情報テーブルに登録されていた場合に、印刷クライアント装置からの印刷要求を受理するとい。

【0010】上記のサーバ装置は、登録されたユーザのパスワード情報を登録したパスワード情報テーブルを管理するユーザ情報管理手段を有し、アクセス制限手段は、印刷クライアント装置からの印刷要求に含まれる印刷依頼プリンタ装置が、プリンタグループ管理手段の管理するプリンタ管理テーブルに登録され、印刷クライアント装置からの印刷要求に含まれるユーザ名が、プリンタアクセス管理テーブルに登録されているか、またはユーザグループ管理手段の管理するユーザグループ管理テーブルに登録され、印刷クライアント装置からの印刷要求に含まれるパスワードが、ユーザ情報管理手段の管理するパスワード情報テーブルに登録されていた場合に、印刷クライアント装置からの印刷要求を受理するとい。

【0011】本発明のプリンタアクセス制御システムは、複数のプリンタと、印刷処理実行不可能なプリンタ装置の情報であるアクセス制限情報を管理するサーバ装置と、サーバ装置からアクセス制限情報を取得し、このアクセス制限情報に基づいて、印刷要求を出力するプリンタ装置を選択する印刷クライアント装置とがネットワークに接続されていることを特徴とする。

【0012】上記の印刷クライアント装置は、所定の間隔毎に前記サーバ装置の管理するアクセス制限情報を取得する取得手段と、取得手段にて取得したアクセス制限情報を記憶する記憶手段とを有するとい。

#### 【0013】

【発明の実施の形態】次に添付図面を参照しながら本発明のプリンタアクセス制御システムに係る実施の形態を詳細に説明する。図1～図9を参照すると本発明のプリンタアクセス制御システムに係る実施の形態が示されている。

【0014】図1には、本発明のプリンタアクセス制御システムに係る第1の実施形態の構成が示されている。図1に示されるように本実施形態は、プリンタ1、プリンタ2、パーソナルコンピュータ（以下、PC装置とい

う) 3、PC装置4、およびサーバ装置10が、LAN/WAN100を介してネットワーク接続されている。サーバ装置10は、PC装置3あるいはPC装置4からのプリンタ情報印刷リクエストに対し、登録されているアクセス制限情報に従って印刷制御を行う。なお、図1に示されたネットワーク構成においては、2台のプリンタとPC装置とが接続された構成となっているが、プリンタ、PC装置、サーバ装置の接続台数はこれに限定されるものではない。

【0015】図2には、サーバ装置10の内部構成のブロック図が示されている。サーバ装置10は、主に、システム制御部20、LAN/WAN通信制御部21、リクエスト処理部22、印刷データ格納部23、ユーザ情報管理部24、印刷処理部25、アクセス制限処理部26、プリンタグループ情報管理部27、およびユーザグループ情報管理部から構成され、各部がシステムバス200により接続されている。

【0016】システム制御部20は、システムバス200を介してメモリ管理等システム全体の基本的制御を行う。

【0017】LAN/WAN通信制御部21は、Ethernetを介した通信の制御を行い、印刷リクエストを受信すると、受信した印刷リクエストをリクエスト処理部22に通知する。また、印刷する場合は、印刷処理部25より印刷データの送信リクエストを受け、データをLAN/WAN100を介してプリンタ1あるいはプリンタ2に送信する。

【0018】リクエスト処理部22は、LAN/WAN通信制御部21で受信した印刷リクエストの通知を受け、ターゲットプリンタ情報、ユーザ情報、あるいはパスワード等の情報を取得する。その後、アクセス制限処理部26に印刷制限のチェック要求信号を送出する。なお、印刷データは、印刷データ格納部23に格納される。

【0019】印刷データ格納部23は、リクエスト処理部22から送信された印刷データを格納する。ユーザ情報管理部24は、登録されたユーザコードおよびパスワードを管理する。図5には、ユーザ情報管理部24のユーザおよびパスワードの管理テーブルの格納例が示されている。

【0020】印刷処理部25は、リクエスト処理部22から入力された印刷リクエストの処理を行う。アクセス制限処理部26は、リクエスト処理部22から入力されたアクセス制限リクエストを受け、アクセス制限情報に従ってプリンタグループ情報管理部27、ユーザ情報管理部24およびユーザグループ情報管理部28の管理情報を使用して印刷制限のチェックを行い、印刷してよいかどうかの結果をリクエスト処理部22に返す。なお、図3には、アクセス制限処理部26のアクセス制限情報についてのプリンタアクセス管理テーブルの格納例

が示されている。

【0021】プリンタグループ情報管理部27は、登録されたプリンタグループを管理する。図4には、プリンタグループ情報管理部27のプリンタグループの管理テーブルの格納例が示されている。

【0022】ユーザグループ情報管理部28は、ユーザグループを管理する。図6には、ユーザグループ情報管理部28におけるユーザグループの管理テーブルの格納例が示されている。

【0023】次に、図7に示されたフローチャートを参照しながら、上記構成の実施形態による動作例を説明する。なお、ここでは、クライアント装置となるPC装置から印刷リクエストを受信し、アクセス制限のチェックを行ってから印刷が実行される処理動作について説明する。

【0024】まず、LAN/WAN通信制御部21は、印刷リクエストが受信されると、リクエスト処理部22に受信した印刷リクエスト情報を通知する。リクエスト処理部22は、印刷リクエスト情報からターゲットプリンタ、ユーザ、あるいはパスワードの情報を取得し、アクセス制限処理部26に印刷の制限をするかどうかの判断を依頼する(ステップS701)。

【0025】次に、アクセス制限処理部26は、リクエスト処理部22から渡されたプリンタ情報を元に、プリンタグループ情報管理部27に対し、プリンタが登録されているプリンタグループ情報を取得するリクエストを通知する。プリンタグループ情報管理部27は、図4に示されるプリンタ管理テーブルを検索し、プリンタが登録されているグループを取得する(ステップS702)。

【0026】アクセス制限処理部26は、プリンタグループがあるかどうかを判断し(ステップS703)、プリンタグループがない場合はリクエスト処理部22に対し、印刷拒否を通知する(ステップS712)。ステップS703において、プリンタグループがあると判断した場合、アクセス制限処理部26は図3に示されるプリンタアクセス管理テーブルのそのプリンタグループの項目に印刷リクエストしたユーザが登録されているか検索する(ステップS704)。

【0027】ステップS704の検索により、ユーザが存在したかどうかを判断し(ステップS705)、ユーザが存在すると判断した場合は、パスワードチェックをユーザ情報管理部24に対し行う。ユーザ情報管理部24は、ユーザ管理テーブルに登録されているパスワードが一致しているかどうかのチェックを行う(ステップS706)。

【0028】ステップS706でパスワードが一致していない場合は、アクセス制限処理部26に一致していないことを通知し、印刷を拒否する。また、ステップS706でパスワードが一致したと判断した場合は、ア

クセス制限処理部26はリクエスト処理部22に対して印刷してもよいと通知し、リクエスト処理部22は、印刷処理部25を使用して印刷を実行する(ステップS707)。

【0029】ステップS705において、ユーザが存在しないか判断した場合は、グループ登録されている可能性があるため、ユーザグループ情報のチェックを行う。アクセス制限処理部26は、ユーザグループ情報管理部28に対してユーザが登録されているユーザグループの取得リクエストを行う。ユーザグループ情報管理部28は、図6に示されるユーザグループ管理テーブルから印刷リクエストしたユーザが含まれるユーザグループを検索する(ステップS708)。

【0030】ステップS708の検索によりユーザグループが存在するか否かを判断し(ステップS709)、ユーザグループが存在しないか判断した場合は、アクセス制限処理部26に対し一致していないことを通知し、印刷を拒否する。

【0031】ステップS709でユーザグループが存在すると判断した場合、アクセス制限処理部26は、プリンタアクセス管理テーブルに登録されているステップS702で検索したグループ内にそのユーザグループが登録されているか検索を行う(ステップS710)。ステップS710の検索の結果、ユーザグループが存在するか否かを判断し(ステップS711)、ユーザグループが存在しないか判断した場合は印刷を拒否する。

【0032】ステップS711において、ユーザグループが存在すると判断した場合は、印刷リクエストしたユーザのパスワードチェックをユーザ情報管理部24に対して行う。ユーザ情報管理部24は、ユーザ管理テーブルに登録されているパスワードが一致しているか否かのチェックを行う(ステップS706)。パスワードが一致していると判断した場合はアクセス制限処理部26に対し一致していないことを通知し、印刷を拒否する。また、ステップS706でパスワードが一致したと判断した場合は、アクセス制限処理部26はリクエスト処理部22に対して印刷してもよいと通知し、リクエスト処理部22は、印刷処理部25を使用して印刷を実行する(ステップS707)。

【0033】以上のように、複数のプリンタのアクセス制限をサーバ装置10上で行えるため、設定作業を効率的に行うことができる。また、アクセス制限のユーザ登録がユーザグループで行うことができる。さらに、ユーザ名およびパスワードでアクセス制限の管理を実行できるため、セキュリティが向上し、操作性が上がる。

【0034】次に、本発明のプリンタアクセス制御システムに係る第2の実施形態について説明する。本実施形態は、システム構成は図1に示された第1の実施形態と同一であるが、PC装置(コンピュータ)3あるいはPC装置4が、ユーザからの印刷リクエストに対し、サー

バ装置10から取得したプリンタアクセス制限情報を元に印刷制御を行うことに特徴を有している。

【0035】図8には、本実施形態のPC装置3およびPC装置4の内部構成を示すブロック図が示されている。このPC装置3およびPC装置4は、主に、システム制御部80、LAN/WAN通信制御部81、アクセス制限情報格納部82、U/I処理部83、印刷処理部84、およびアクセス制限処理部85から構成され、各部がシステムバス800により接続されている。

【0036】システム制御部80は、システムバス800を介してメモリ管理等システム全体の基本的制御を行う。

【0037】LAN/WAN通信制御部81は、Ethernetを介した通信の制御を行い、プリンタ1あるいはプリンタ2に対しての印刷指示、あるいはサーバ装置10からのプリンタアクセス制限情報の取得を行う。

【0038】アクセス制限情報格納部82は、サーバ装置10から取得したプリンタアクセス制限情報を格納する。アクセス制限情報はアクセス不可能なプリンタの一覧をテーブルで持つ。

【0039】U/I処理部83は、ユーザからの印刷指示の処理を受け、印刷処理部84に印刷指示を行う。

【0040】印刷処理部84は、印刷処理を行う。その際、アクセス制限処理部85に対しアクセス制限があるか否かの問い合わせを行う。

【0041】アクセス制限処理部85は、アクセス制限情報格納部82よりプリンタアクセス制限情報を取得しアクセス制限のチェックを行う。

【0042】次に、図9に示されたフローチャートを参照しながら、上記構成の実施形態による動作例を説明する。

【0043】まず、U/I処理部83でユーザからの印刷指示を受け取ると、U/I処理部83は印刷処理部84に対して、印刷データ及びターゲットプリンタの情報を通知する(ステップS901)。

【0044】次に、印刷処理部84は、アクセス制限処理部85に対して印刷可能なプリンタか否かの問い合わせを行う(ステップS902)。

【0045】次に、アクセス制限処理部85は、アクセス制限情報をサーバ装置10から取得したか否かを判断し(ステップS903)、取得していないと判断した場合は、サーバ装置10からアクセス制限情報を取得する(ステップS905)。

【0046】また、ステップS903で、サーバ装置10からアクセス制限情報を既に取得していると判断した場合には、アクセス制限情報を取得してから予め設定された一定時間が経過したか否か、つまりプリンタアクセス制限が古くなっているか否かを判断する(ステップS904)。

【0047】ステップS904において、アクセス制限

情報を取得してから予め設定された一定時間が経過していないと判断した場合は、次に印刷可能なプリンタか否かを判断し(ステップS906)、アクセス制限処理部95から印刷可能という指示が入力された場合は印刷を実行する(ステップS907)。

【0048】ステップS904において、アクセス制限情報を取得してから予め設定された一定時間が経過していると判断した場合は、サーバ装置10からアクセス制限情報を取得して(ステップS905)、ステップS906に移る。また、ステップS906でアクセス制限処理部95からアクセス制限対象であり、印刷不可という指示が入力された場合は、印刷を中止させる。

【0049】上述のように、サーバ装置経由以外の印刷処理に対してもプリンタへのアクセス制限を行うことが可能となるため、アクセス制限の適用範囲を広げることができる。

【0050】なお、上述した実施形態は、本発明の好適な実施の形態である。但し、これに限定されるものではなく、本発明の要旨を逸脱しない範囲内において種々変形実施が可能である。

#### 【0051】

【発明の効果】ネットワーク接続されたサーバ装置にアクセス制限処理手段、プリンタグループ管理手段あるいはユーザグループ管理手段が搭載されており、ネットワーク上の複数のプリンタのアクセス制限をサーバ上で行うことができるため、アクセス条件の設定作業を効率よく行うことができる。

【0052】また、アクセス制限のユーザ登録をユーザグループで行うことができるため、作業効率が向上させることができる。

【0053】さらに、ユーザ名およびパスワードでアクセス制限の管理を行うことができるため、セキュリティおよび操作性を向上させることができる。

【0054】また、サーバ装置が印刷処理実行不可能なプリンタ装置の情報であるアクセス制限情報を管理し、印刷クライアント装置がサーバ装置からのアクセス制限情報を取得し、印刷要求を出力するプリンタ装置を選

択することにより、サーバ装置経由の印刷処理に関してもアクセス制限を実行させることが可能となり、アクセス制限の適用範囲を拡張させることができる。

#### 【図面の簡単な説明】

【図1】本発明のプリンタアクセス制御システムの構成例を示す図である。

【図2】本発明に係るサーバ装置の内部構成例を示す機能ブロック図である。

【図3】プリンタアクセス管理テーブルの格納例を示す図である。

【図4】プリンタ管理テーブルの格納例を示す図である。

【図5】ユーザ管理テーブルの格納例を示す図である。

【図6】ユーザグループ管理テーブルの格納例を示す図である。

【図7】本発明のプリンタアクセス制御システムの制御例を示すフロー図である。

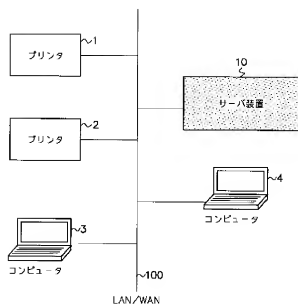
【図8】本発明に係るPC装置の内部構成例を示す機能ブロック図である。

【図9】本発明のプリンタアクセス制御システムにかかるPC装置の制御例を示すフロー図である。

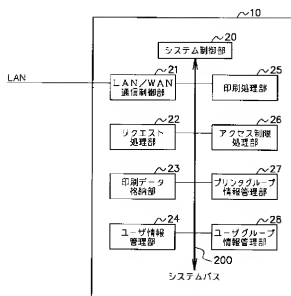
#### 【符号の説明】

- 1、2 プリンタ
- 3、4 PC装置(コンピュータ)
- 10 サーバ装置
- 20、80 システム制御部
- 21、81 LAN/WAN通信制御部
- 22 リクエスト処理部
- 23 印刷データ格納部
- 24 ユーザ情報管理部
- 25、84 印刷処理部
- 26、85 アクセス制限処理部
- 27 プリンタグループ情報管理部
- 28 ユーザグループ管理部
- 82 アクセス制限情報格納部
- 83 UI処理部

【図1】



【図2】



【図3】

プリンタグループ	ユーザ/ユーザグループ
Group A	watanabe
	suzuki
	saitoh
	usergroup 1
Group B	morita
	yamaguchi
	suzuki

【図4】

グループ	プリンタ
Group A	Printer A
	Printer B
	Printer C
	Printer D
	Printer E
Group B	Printer Color A
	Printer Color B
	Printer Color C

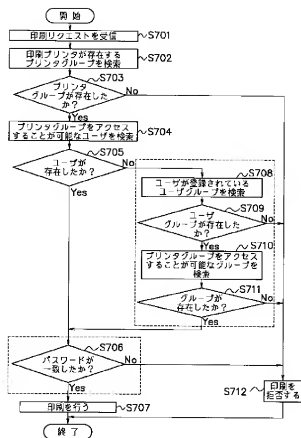
【図5】

ユーザ	パスワード
watanabe	123
suzuki	1234
saitoh	1235
tanaka	1236
morita	1237
yamaguchi	1238
saitoh	1239

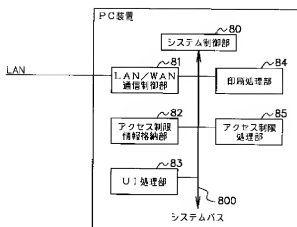
【図6】

プリンタグループ	ユーザ
UserGroup 1	yamaguchi
	morita
	saitoh
UserGroup 2	morita
	suzuki

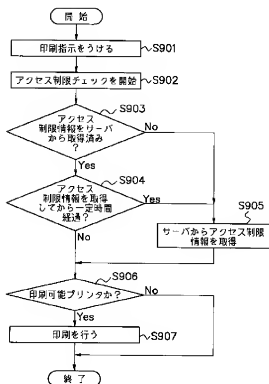
【図7】



【図8】



【図9】





**PAT-NO:** JP02001014123A  
**DOCUMENT-IDENTIFIER:** JP 2001014123 A  
**TITLE:** PRINTER ACCESS CONTROL  
SYSTEM  
**PUBN-DATE:** January 19, 2001

**INVENTOR-INFORMATION:**

NAME	COUNTRY
WATANABE, YOSHIAKI	N/A

**ASSIGNEE-INFORMATION:**

NAME	COUNTRY
RICOH CO LTD	N/A

**APPL-NO:** JP11183407  
**APPL-DATE:** June 29, 1999

**INT-CL (IPC):** G06F003/12 , B41J029/38 , G06F013/00

**ABSTRACT:**

**PROBLEM TO BE SOLVED:** To easily set the access restrictions of plural printers which are connected by a network by allowing a print-requested printer to reject a print request from a print client device under a specific condition.

**SOLUTION:** An access restriction processing part 26 informs a printer group information management part 27 of a request to acquire printer group information where a printer is registered according to printer information passed from a request process part 22. The printer group information

management part 27 performs retrieval from a printer management table to acquire the group where the printer is registered and informs the request process part 22 of print rejection when no printer group is found. Further, a user information management part 24 checks whether or not a password registered in a user management table is matched, and informs the access restriction process part 26 of no match in such a case and then rejects the printing.

COPYRIGHT: (C)2001,JPO

JAPANESE

[JP,2001-014123,A]

CLAIMS DETAILED DESCRIPTION TECHNICAL  
FIELD PRIOR ART EFFECT OF THE INVENTION  
TECHNICAL PROBLEM MEANS DESCRIPTION OF  
DRAWINGS DRAWINGS

[Translation done.]

\* NOTICES \*

**JPO and INPIT are not responsible for  
any  
damages caused by the use of this  
translation.**

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

## DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to the printer access control system of the printer by which network connection was carried out.

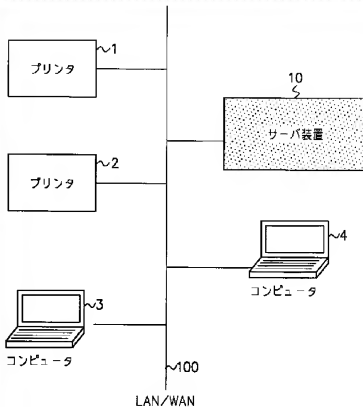
[0002]

[Description of the Prior Art]The access control of the printer conventionally connected to the network built by two or more workstations as a network printer was specified by the existence of the right to access which determines to which user use of a printer is permitted, for example. However, in this system control, the fine conditions for every user permitted were not able to be set up.

[0003]As a method of solving this problem, in JP,8-31468, A. The network printer device which performs finer control for every user is proposed by registering the printer access information which registers a user name into a printer as information which shows the right to access and for which the record output for every user of the is simultaneously restricted to it.

[0004]

Drawing selection **Representative draw**



[Translation done.]

[Problem(s) to be Solved by the Invention]However, in this network printer device. In performing access restriction on the same conditions, two or more printers by which network connection was carried out, In order to have to perform the same operation to each printer and to have to do the operational input work of change etc. to each printer also in changing an access condition etc., time and effort was taken very much and the problem that working efficiency worsened had occurred.

[0005]When access restriction was performed from on the server apparatus which exists on a network, it also had the problem that only printing via a server could perform access restriction.

[0006]An object of this invention is to provide the printer access control system which can cancel the conventional fault and can set up easily the access restriction of two or more printers by which network connection was carried out.

[0007]

[Means for Solving the Problem]This invention in order to attain this purpose a printer access control system of this invention, A server apparatus which transmits print data which accumulated a printing client device which outputs a printing demand, and print data contained in a printing demand from a printing client device, and were accumulated in a printer, A printer access control system by which a printer which carries out the record output of the print data sent from a server apparatus by a recording device at a paper was connected to a network is characterized by comprising: A printer group management tool which manages a printer management table which a server apparatus carried out grouping of two or more printers connected to a network, and was registered.

A printer access control table which registered User Information for every group of a printer is managed, A printing request printer included in a printing demand from a printing client device, When not contained in a printer management table which a printer group management tool manages, Or an access-restriction means to refuse a printing demand from a printing client device when a user name contained in a printing demand from a printing client device is not registered into a printer access control table.

[0008]Have the above-mentioned server apparatus and an user-group management tool which manages an user-group management table which carried out grouping of two or more user names, and registered them an access-restriction means, A printing request printer included in a printing demand from a printing client device, When not contained in a printer management table which a printer group management tool manages, Or when a user name contained

in a printing demand from a printing client device is not registered into a printer access control table and an user-group management table, it is good to refuse a printing demand from a printing client device.

[0009]Have the above-mentioned server apparatus and the User Information management tool which manages a password information table which registered a user's registered password information an access-restriction means, A printing request printer included in a printing demand from a printing client device, It registers with a printer management table which a printer group management tool manages, A user name contained in a printing demand from a printing client device is registered into a printer access control table, When a password contained in a printing demand from a printing client device is registered into a password information table which the User Information management tool manages, it is good to receive a printing demand from a printing client device.

[0010]Have the above-mentioned server apparatus and the User Information management tool which manages a password information table which registered a user's registered password information an access-restriction means, A printing request printer included in a printing demand from a printing client device, It registers with a printer management table which a printer group management tool manages, A user name contained in a printing demand from a printing client device. [ whether it registers with a printer access control table, and ] Or it registers with an user-group management table which an user-group management tool manages, When a password contained in a printing demand from a printing client device is registered into a password information table which the User Information management tool manages, it is good to receive a printing demand from a printing client device.

[0011]A server apparatus which manages access restriction information whose printer access control systems of this invention are two or more printers and the information on a printer in which printing job execution is impossible, Access restriction information is acquired from a server apparatus, and a printing client device which chooses a printer which outputs a printing demand is connected to a network based on this access restriction information.

[0012]The above-mentioned printing client device is good to have an acquisition means which acquires access restriction information which said server apparatus manages for every predetermined interval, and a memory measure which memorizes access restriction information acquired in an acquisition means.

[0013]

[Embodiment of the Invention]Next, the embodiment

concerning the printer access control system of this invention is described in detail, referring to an accompanying drawing. Reference of drawing 1 - drawing 9 shows the embodiment concerning the printer access control system of this invention.

[0014]The composition of a 1st embodiment concerning the printer access control system of this invention is shown in drawing 1. As shown in drawing 1, as for this embodiment, network connection of the printer 1, the printer 2, the personal computer (henceforth a PC device) 3, PC device 4, and the server apparatus 10 is carried out via LAN/WAN100. The server apparatus 10 performs printing controlling according to the access restriction information registered to the printer information print request from PC device 3 or PC device 4. In the network composition shown in drawing 1, although the composition to which two printers and PC devices were connected is taken, the number of connection pedestals of a printer, a PC device, and a server apparatus is not limited to this.

[0015]The block diagram of the internal configuration of the server apparatus 10 is shown in drawing 2. The server apparatus 10 mainly, It comprises the system control part 20, the LAN/WAN communication control part 21, the request processing part 22, the print data storing part 23, the User Information Management Department 24, the printing job part 25, the access-restriction treating part 26, the printer group Research and Data Processing Department 27, and the user-group Research and Data Processing Department, Each part is connected by the system bath 200.

[0016]The system control part 20 performs fundamental control of the whole system, such as memory management, via the system bath 200.

[0017]If the LAN/WAN communication control part 21 controls communication through Ethernet and a print request is received, it will notify the print request which received to the request processing part 22. When printing, the send request of print data is received from the printing job part 25, and data is transmitted to the printer 1 or the printer 2 via LAN/WAN100.

[0018]The request processing part 22 receives the notice of the print request which received by the LAN/WAN communication control part 21, and acquires the information on target printer information, User Information, or a password. Then, the check request signal of printing restrictions is sent out to the access-restriction treating part 26. Print data are stored in the print data storing part 23.

[0019]The print data storing part 23 stores the print data transmitted from the request processing part 22. The User Information Management Department 24 manages the user code and password which were registered. The user of the

User Information Management Department 24 and the example of storing of the management table of a password are shown in [drawing 5](#).

[0020]The printing job part 25 processes the print request inputted from the request processing part 22. The access-restriction treating part 26 receives the access-restriction request inputted from the request processing part 22, According to access restriction information, printing restrictions are checked using the management information of the printer group Research and Data Processing Department 27, the User Information Management Department 24, and the user-group Research and Data Processing Department 28, and the result of whether to print is returned to the request processing part 22. The example of storing of the printer access control table about the access restriction information of the access-restriction treating part 26 is shown in [drawing 3](#).

[0021]The printer group Research and Data Processing Department 27 manages the registered printer group. The example of storing of the management table of the printer group of the printer group Research and Data Processing Department 27 is shown in [drawing 4](#).

[0022]The user-group Research and Data Processing Department 28 manages an user group. The example of storing of the management table of the user group in the user-group Research and Data Processing Department 28 is shown in [drawing 6](#).

[0023]Next, the example of operation by the embodiment of the above-mentioned composition is explained, referring to the flow chart shown in [drawing 7](#). Here, a print request is received from the PC device used as a client apparatus, and after checking access restriction, the processing operation by which printing is performed is explained.

[0024]First, the LAN/WAN communication control part 21 will notify the print request information received to the request processing part 22, if a print request is received. The request processing part 22 acquires the information on a target printer, a user, or a password from print request information, and requests judgment whether printing is restricted to the access-restriction treating part 26 (Step S701).

[0025]Next, the access-restriction treating part 26 notifies the request which acquires the printer group information into which the printer is registered to the printer group Research and Data Processing Department 27 based on the printer information passed from the request processing part 22. The printer group Research and Data Processing Department 27 searches the printer management table shown in [drawing 4](#), and the group by whom the printer is

registered is acquired (Step S702).

[0026]It judges whether the access-restriction treating part 26 has a printer group (Step S703), and when there is no printer group, printing refusal is notified to the request processing part 22 (Step S712). In Step S703, when it is judged that there is a printer group, the access control treating part 26 searches whether the user who did the print request to the item of the printer group of the printer access control table shown in [drawing 3](#) is registered (Step S704).

[0027]By search of Step S704, when it judges whether the user existed or not (Step S705) and it is judged that a user exists, a password check is performed to the User Information Management Department 24. The User Information Management Department 24 confirms whether the password registered into the user management table is in agreement (Step S706).

[0028]When the password is not in agreement at Step S706, it reports that it is not in agreement to the access-restriction treating part 26, and printing is refused. When it is judged that the password was in agreement at Step S706, it reports that the access-restriction treating part 26 may be printed to the request processing part 22, and the request processing part 22 performs printing using the printing job part 25 (Step S707).

[0029]In Step S705, since group registration may be carried out when it is judged that a user does not exist, user-group information is checked. The access-restriction treating part 26 performs the acquisition request of the user group which is received user-group Research and Data Processing Department 28 and into which the user is registered. The user-group Research and Data Processing Department 28 searches the user group in which the user who did the print request from the user-group management table shown in [drawing 6](#) is contained (Step S708).

[0030]When it judges whether an user group exists by search of Step S708 (Step S709) and it is judged that an user group does not exist, it reports that it is not in agreement to the access-restriction treating part 26, and printing is refused.

[0031]When it is judged that an user group exists at Step S709, the user group is registered into the group who is at Step S702 registered into the printer access control table, and searched, or the access-restriction treating part 26 searches (Step S710). As a result of search of Step S710, when it judges whether an user group exists (Step S711) and it is judged that an user group does not exist, printing is refused.

[0032]In Step S711, when it is judged that an user group exists, a user's password check which carried out the print request is performed to the User Information Management



Department 24. The User Information Management Department 24 confirms whether the password registered into the user management table is in agreement (Step S706), when it is judged that the password is in agreement, it reports that it is not in agreement to the access-restriction treating part 26, and it refuses printing. When it is judged that the password was in agreement at Step S706, it reports that the access-restriction treating part 26 may be printed to the request processing part 22, and the request processing part 22 performs printing using the printing job part 25 (Step S707).

[0033]Above, like, since access restriction of two or more printers can be performed on the server apparatus 10, setting out can be performed efficiently. User registration of access restriction can carry out by an user group. Since management of access restriction can be performed with a user name and a password, security improves and operativity goes up.

[0034]Next, a 2nd embodiment concerning the printer access control system of this invention is described. This embodiment has the feature to perform printing controlling based on the printer access restriction information which PC device (computer) 3 or PC device 4 acquired from the server apparatus 10 to the print request from a user, although the system configuration is the same as that of a 1st embodiment shown in [drawing 1](#).

[0035]The block diagram showing the internal configuration of PC device 3 of this embodiment and PC device 4 is shown in [drawing 8](#). This PC device 3 and PC device 4 mainly comprise the system control part 80, the LAN/WAN communication control part 81, the access-restriction-information storage 82, the UI treating part 83, the printing job part 84, and the access-restriction treating part 85, and each part is connected by the system bath 800.

[0036]The system control part 80 performs fundamental control of the whole system, such as memory management, via the system bath 800.

[0037]The LAN/WAN communication control part 81 controls communication through Ethernet, and acquires the printing directions to the printer 1 or the printer 2, or the printer access restriction information from the server apparatus 10.

[0038]The access-restriction-information storage 82 stores the printer access restriction information acquired from the server apparatus 10. Access restriction information has on a table a list of the printer which cannot be accessed.

[0039]The UI treating part 83 receives processing of the printing directions from a user, and performs printing directions in the printing job part 84.

[0040]The printing job part 84 performs a printing job. In

that case, it is asked whether there is any access restriction to the access-restriction treating part 85.

[0041]The access-restriction treating part 85 acquires printer access restriction information from the access-restriction-information storage 82, and checks access restriction.

[0042]Next, the example of operation by the embodiment of the above-mentioned composition is explained, referring to the flow chart shown in [drawing 9](#).

[0043]First, if the printing directions from a user are received by the UI treating part 83, the UI treating part 83 will notify the information on print data and a target printer to the printing job part 84 (Step S901).

[0044]Next, the printing job part 84 asks that it is a printer which can print to the access-restriction treating part 85 (Step S902).

[0045]Next, when it is judged that the access-restriction treating part 85 judges whether access restriction information was acquired from the server apparatus 10 (Step S903), and does not acquire, access restriction information is acquired from the server apparatus 10 (Step S905).

[0046]When it is judged at Step S903 that access restriction information is already acquired from the server apparatus 10, after acquiring access restriction information, it is judged whether whether the fixed time set up beforehand having passed and printer access restriction that is, are old (Step S904).

[0047]After acquiring access restriction information in Step S904, when it is judged that the fixed time set up beforehand has not passed, Next, it judges whether it is a printer which can print (Step S906), and printing is performed when directions that printing is possible are inputted from the access-restriction treating part 95 (Step S907).

[0048]In Step S904, after acquiring access restriction information, when it is judged that the fixed time set up beforehand has passed, access restriction information is acquired from the server apparatus 10 (Step S905), and it moves to Step S906. Printing is stopped, when it is an access-restriction object and directions that printing is impossible are inputted from the access-restriction treating part 95 at Step S906.

[0049]As mentioned above, since it becomes possible to perform access restriction to a printer also to printing jobs other than via a server apparatus, the scope of access restriction can be extended.

[0050]The embodiment mentioned above is a suitable embodiment of this invention. However, modification implementation is variously possible within limits which do not deviate not from the thing limited to this but from the gist of this invention.

[0051]

[Effect of the Invention]The access-restriction processing means, the printer group management tool, or the user-group management tool is carried in the server apparatus by which network connection was carried out, Since access restriction of two or more printers on a network can be performed on a server, setting out of an access condition can be performed efficiently.

[0052]Since access restriction can be registered as a user by an user group, working efficiency can be raised.

[0053]Since access restriction is manageable with a user name and a password, security and operativity can be raised.

[0054]The access restriction information which is information on the printer which a server apparatus cannot printing job perform is managed, It can become possible to perform access restriction also about the printing job via a server apparatus, and the scope of access restriction can be made to extend by a printing client device's acquiring this access restriction information from a server apparatus, and choosing the printer which outputs a printing demand.

---

[Translation done.]